ANNEX III

THE SECRETARY OF STATE
WASHINGTON

February 22, 2016

Dear Commissioner Jourová,

I am pleased we have reached an understanding on the European Union-United States Privacy Shield that will include an Ombudsperson mechanism through which authorities in the EU will be able to submit requests on behalf of EU individuals regarding U.S. signals intelligence practices.

On January 17, 2014, President Barack Obama announced important intelligence reforms included in Presidential Policy Directive 28 (PPD-28). Under PPD-28, I designated Under Secretary of State Catherine A. Novelli, who also serves as Senior Coordinator for International Information Technology Diplomacy, as our point of contact for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. Building on this role, I have established a Privacy Shield Ombudsperson mechanism in accordance with the terms set out in Annex A. I have directed Under Secretary Novelli to perform this function. Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me.

I have directed my staff to devote the necessary resources to implement this new Ombudsperson mechanism, and am confident it will be an effective means to address EU individuals' concerns.

Sincerely,

John F. Kerry

EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence

In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with Presidential Policy Directive 28 (PPD-28), regarding signals intelligence.

On January 17, 2014, President Obama gave a speech announcing important intelligence reforms. In that speech, he pointed out that "[o]ur efforts help protect not only our nation, but our friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too." President Obama announced the issuance of a new presidential directive—PPD-28—to "clearly prescribe what we do, and do not do, when it comes to our overseas surveillance."

Section 4(d) of PPD-28 directs the Secretary of State to designate a "Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) "to ... serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States." As of January 2015, Under Secretary C. Novelli has served as the Senior Coordinator.

This Memorandum describes a new mechanism that the Senior Coordinator will follow to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), "Derogations,"[1] or "Possible Future Derogations,"[2] through

[1] "Derogations" in this context mean a commercial transfer or transfers that take place on the condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

[2] "Possible Future Derogations" in this context mean a commercial transfer or transfers that take place on one of the following conditions, to the extent the condition constitutes lawful grounds for transfers of personal data from the EU to the U.S.: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate

established avenues under applicable United States laws and policy, and the response to those requests.

1. **The Privacy Shield Ombudsperson.** The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. (Hereinafter, the Coordinator and any officials performing such duties will be referred to as "Privacy Shield Ombudsperson.") The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Under Secretary reports directly to the Secretary of State, and is independent from the Intelligence Community.

2. **Effective Coordination.** The Privacy Shield Ombudsperson will be able to effectively use and coordinate with the mechanisms and officials described below, in order to ensure appropriate response to communications from submitting EU individual complaint handing body.

    a. The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers.

    b. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests under Section 3(b).

    c. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

---

safeguards; or (b) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (c) where a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data.

3. **Submitting Requests.**

   a. A request will initially be submitted to the Member States bodies competent for the oversight of national security services. The EU reserves the possibility to designate a centralized EU individual complaint handling body to which a request can also be submitted (hereafter together or alternatively: the "EU individual complaint handling body").

   b. The EU individual complaint handling body will ensure, in compliance with the following actions, that the request is complete:

      (i) Verifying the identity of the individual, and that the individual is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organization.
      (ii) Ensuring the request is made in writing, and that it contains the following basic information:
         - any information that forms the basis for the request,
         - the nature of information or relief sought,
         - the United States Government entities believed to be involved, if any, and
         - the other measures pursued to obtain the information or relief requested and the response received through those other measures.
      (iii) Verifying that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to the Privacy Shield, SCCs, BCRs, Derogations, or Possible Future Derogations.
      (iv) Making an initial determination that the request is not frivolous, vexatious, or made in bad faith.

   c. To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester's data has in fact been accessed by the United States Government through signal intelligence activities.

4. **Commitments to Communicate with Submitting EU Individual Complaint Handling Body.**

   a. The Privacy Shield Ombudsperson will acknowledge receipt of the request to the submitting EU individual complaint handling body.

   b. The Privacy Shield Ombudsperson will conduct an initial review to verify that the request has been completed in conformance with Section 3(b). If the Privacy Shield Ombudsperson notes any deficiencies or has any questions regarding the completion of the request, the Privacy Shield Ombudsperson will seek to address and resolve those concerns with the submitting EU individual complaint handling body.

c. If, to facilitate appropriate processing of the request, the Privacy Shield Ombudsperson needs more information about the request, or if specific action is needed to be taken by the individual who originally submitted the request, the Privacy Shield Ombudsperson will so inform the submitting EU individual complaint handling body.

d. The Privacy Shield Ombudsperson will track the status of requests and provide updates as appropriate to the submitting EU individual complaint handling body.

e. Once a request has been completed as described in Section 3 of this Memorandum, the Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.

f. The Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.

g. Commitments in this Memorandum will not apply to general claims that the EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the European Commission any adjustments that may be appropriate to address the situation.

5. **Requests for Information.** Requests for access to United States Government records may be made and processed under the Freedom of Information Act (FOIA).

a. FOIA provides a means for any person to seek access to existing federal agency records, regardless of the nationality of the requester. This statute is codified in the United States Code at 5 U.S.C. § 552. The statute, together with additional information about FOIA, is available at www.FOIA.gov and http://www.justice.gov/oip/foia-resources. Each agency has a Chief FOIA Officer, and has provided information on its public website about how to submit a FOIA request to the agency. Agencies have processes for consulting with one another on FOIA requests that involve records held by another agency.

b. By way of example:

   (i) The Office of the Director of National Intelligence (ODNI) has established the ODNI FOIA Portal for the ODNI: http://www.dni.gov/index.php/about-this-site/foia. This portal provides information on submitting a request, checking on the status of an existing request, and accessing information that has been released and published by the ODNI under FOIA. The ODNI FOIA Portal includes links to other FOIA websites for IC elements: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

   (ii) The Department of Justice's Office of Information Policy provides comprehensive information about FOIA: http://www.justice.gov/oip. This includes not only information about submitting a FOIA request to the Department of Justice, but also provides guidance to the United States government on interpreting and applying FOIA requirements.

c. Under FOIA, access to government records is subject to certain enumerated exemptions. These include limits on access to classified national security information, personal information of third parties, and information concerning law enforcement investigations, and are comparable to the limitations imposed by each EU Member State with its own information access law. These limitations apply equally to Americans and non-Americans.

d. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a *de novo* determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified. Although no monetary damages are available, courts can award attorney's fees.

6. **Requests for Further Action.** A request alleging violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance as described below.

a. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions.

   (i) The Inspector General Act of 1978, as amended, statutorily established the Federal Inspectors General (IG) as independent and objective units within most agencies whose duties are to combat waste, fraud, and abuse in the programs and operations of their respective agencies. To this end, each IG is responsible for conducting audits and investigations relating to the programs and operations of its agency. Additionally, IGs provide leadership and coordination and recommend policies for activities designed to promote economy, efficiency, and effectiveness, and prevent and detect fraud and abuse, in agency programs and operations.

   (ii) Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. A number of Inspector General reports about intelligence programs have been publicly released.

   (iii) By way of example:

   - The Office of the Inspector General of the Intelligence Community (IC IG) was established pursuant to Section 405 of the Intelligence Authorization Act of Fiscal Year 2010. The IC IG is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies. The IC IG is authorized to investigate complaints or information concerning allegations of a violation of law, rule, regulation, waste, fraud, abuse of authority, or a substantial or specific danger to public health and safety in connection with ODNI and/or IC intelligence programs and activities. The IC IG provides information on how to contact the IC IG directly to submit a report: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

   - The Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs. The OIG has jurisdiction over all complaints of misconduct against Department of Justice employees, including the Federal Bureau of Investigation; Drug Enforcement Administration; Federal Bureau of Prisons; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; United States Attorneys Offices; and employees who work in other

Divisions or Offices in the Department of Justice. (The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorney's authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility.) In addition, section 1001 of the USA Patriot Act, signed into law on October 26, 2001, directs the Inspector General to review information and receive complaints alleging abuses of civil rights and civil liberties by Department of Justice employees. The OIG maintains a public website – https://www.oig.justice.gov – which includes a "Hotline" for submitting complaints – https://www.oig.justice.gov/hotline/index.htm.

b. Privacy and Civil Liberties offices and entities in the United States Government also have relevant responsibilities. By way of example:

(i) Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified in the United States Code at 42 U.S.C. § 2000-ee1, establishes privacy and civil liberties officers at certain departments and agencies (including the Department of State, Department of Justice, and ODNI). Section 803 specifies that these privacy and civil liberties officers will serve as the principal advisor to, among other things, ensure that such department, agency, or element has adequate procedures to address complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties.

(ii) The ODNI's Civil Liberties and Privacy Office (ODNI CLPO) is led by the ODNI Civil Liberties Protection Officer, a position established by the National Security Act of 1948, as amended. The duties of the ODNI CLPO include ensuring that the policies and procedures of the elements of the Intelligence Community include adequate protections for privacy and civil liberties, and reviewing and investigating complaints alleging abuse or violation of civil liberties and privacy in ODNI programs and activities. The ODNI CLPO provides information to the public on its website, including instructions for how to submit a complaint: www.dni.gov/clpo. If the ODNI CLPO receives a privacy or civil liberties complaint involving IC programs and activities, it will coordinate with other IC elements on how that complaint should be further processed within the IC. Note that the National Security Agency (NSA) also has a Civil Liberties and Privacy Office, which provides information about its responsibilities on its website – https://www.nsa.gov/civil_liberties/. If information indicates that an agency is out of compliance with privacy requirements (*e.g.*, a requirement under Section 4 of PPD-28), then agencies have compliance mechanisms to review and remedy the incident. Agencies are required to report compliance incidents under PPD-28 to the ODNI.

(iii) The Office of Privacy and Civil Liberties (OPCL) at the Department of Justice supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties. OPCL provides information to the public about its responsibilities at http://www.justice.gov/opcl.

(iv) According to 42 U.S.C. § 2000ee *et seq.*, the Privacy and Civil Liberties Oversight Board shall continually review (i) the policies and procedures, as well as their implementation, of the departments, agencies and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected, and (ii) other actions by the executive branch relating to such efforts to determine whether such actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties. It shall receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified at 42 U.S.C. § 2000ee-1, directs the privacy and civil liberties officers of eight federal agencies (including the Secretary of Defense, Secretary of Homeland Security, Director of National Intelligence, and Director of the Central Intelligence Agency), and any additional agency designated by the Board, to submit periodic reports to the PCLOB, including the number, nature, and disposition of the complaints received by the respective agency for alleged violations. The PCLOB's enabling statute directs the Board to receive these reports and, when appropriate, make recommendations to the privacy and civil liberties officers regarding their activities.